PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-054744
(43)Date of publication of application : 19.02.2004

(51)Int.Cl. G06F 12/14
G06F 17/60
H04L 9/08
H04N 7/173

(21)Application number : 2002-213700
(22)Date of filing : 23.07.2002

(71)Applicant : SONY CORP
(72)Inventor : KITATANI YOSHIMICHI
KURIYA YUKINOBU

(54) INFORMATION PROCESSORINFORMATION PROCESSING METHOD AND COMPUTER PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a device and a method that realize improved processing for a content audition in a content use structure based on use right information about content.
SOLUTION: A client acquires default use right information in registration processing to a license serverand determines whether or not to permit content reproduction from the default use right information in audition processing without content purchase processing. Audition-permitted clients are limited to clients having the default use right information via registration processing to the license serverso that audition data are protected against disorderly flooding.

CLAIMS

[Claim(s)]
[Claim 1]
It is an information processor which performs decoding of enciphered contentand regeneration
As contents playback conditionsit has a control means which performs regeneration based on this contents right-of-use information with reference to contents right-of-use information
Said control means
When reproducing purchase contentsa reproduction propriety judging based on description of right-of-use information corresponding to contents is performed

An information processor having the composition which performs a reproduction propriety judging based on description of default right-of-use information as contents right-of-use information corresponding to audition processing on the occasion of audition processing of contents.

[Claim 2]

Said default right-of-use information has right permit information of contents playback based on a preset value of an audition flag set as a contents file

Said control means

The information processor according to claim 1 being the composition of verifying an audition flag added to contents for an audition on the occasion of audition processing of contentsand judging reproductive propriety based on this verification result.

[Claim 3]

Said information processor

Purchase reproduction execution application applied to purchase regeneration of contents and audition processing execution application applied to audition processing of contents are stored

Said control means

The information processor according to claim 1 being the composition of choosing and performing either said purchase reproduction execution application or audition processing execution application based on a startup file to input from the outside.

[Claim 4]

Said information processor

Purchase reproduction execution application applied to purchase regeneration of contents and audition processing execution application applied to audition processing of contents are stored

Said control means

The information processor according to claim 1 being the composition of choosing and performing either said purchase reproduction execution application or audition processing execution application based on an extension set as a startup file to input from the outside.

[Claim 5]

Said enciphered content

It is the contents enciphered by the contents key Kcand said contents key Kc is a key acquirable only by application of a key acquirable by decoding of validation key blocks (EKB) provided with the application of validation key-blocks (EKB) distribution tree composition

Said control means

The information processor according to claim 1 being the composition of performing contents key acquisition processing by decoding processing of said validation key blocks (EKB).

[Claim 6]

It is an information processor as a license server which publishes contents right-of-use information over a client which performs contents playback

Service information which stored validation key blocks (EKB) which contain a device node key (DNK) which is needed in the case of decoding processing of enciphered content according to a registry request from a client
An information processor having the composition which performs processing which generates default right-of-use information as contents right-of-use information applied to a reproduction propriety judging in audition processing of contents in a clientand is published to a client.
[Claim 7]
Said information processor
The information processor according to claim 6 having the composition which performs processing which generates default right-of-use information that right permit information of contents playback based on a preset value of an audition flag set as a contents file was stored.
[Claim 8]
It is an information processing method which performs decoding of enciphered contentand regeneration
As contents playback conditionsit has a contents playback control step which performs regeneration based on this contents right-of-use information with reference to contents right-of-use information
Said contents playback control step is further
A step which judges whether it is regeneration of purchase contentsor it is audition processing of contents
A reproduction propriety decision processing step based on description of right-of-use information corresponding to contents which perform as conditions that it is regeneration of purchase contents
An information processing method containing a reproduction propriety decision processing step based on description of default right-of-use information as contents right-of-use information corresponding to audition processing which performs as conditions that it is audition processing of contents.
[Claim 9]
Said default right-of-use information has right permit information of contents playback based on a preset value of an audition flag set as a contents file
Said contents playback control step
The information processing method according to claim 8 verifying an audition flag added to contents for an audition on the occasion of audition processing of contentsand judging reproductive propriety based on this verification result.
[Claim 10]
Said information processing method is further
It has a selection step which chooses either purchase reproduction execution application or audition processing execution application from the exterior based on a startup file to input
Said contents playback control step
The information processing method according to claim 8 performing according to AUPURIKESHON selected in said selection step.

[Claim 11]
Said information processing method is further
A step which distinguishes an extension of a startup file inputted from the outside
Based on an extension of a distinguished startup fileit has a selection step which chooses either purchase reproduction execution application or audition processing execution application
Said contents playback control step
The information processing method according to claim 8 performing according to AUPURIKESHON selected in said selection step.
[Claim 12]
Said enciphered content
It is the contents enciphered by the contents key Kcand said contents key Kc is a key acquirable only by application of a key acquirable by decoding of validation key blocks (EKB) provided with the application of validation key-blocks (EKB) distribution tree composition
Said contents playback control step
The information processing method according to claim 8 containing a step which performs contents key acquisition processing by decoding processing of said validation key blocks (EKB).
[Claim 13]
It is an information processing method in a license server which publishes contents right-of-use information over a client which performs contents playback
A step which receives a registry request from a client
Service information which stored validation key blocks (EKB) which contain a device node key (DNK) which is needed in the case of decoding processing of enciphered content according to reception of said registry requestA step which generates default right-of-use information as contents right-of-use information applied to a reproduction propriety judging in audition processing of contents in a client
A step which transmits generated service information and default right-of-use information to a client
A ****(ing) information processing method.
[Claim 14]
In said information processing method
The information processing method according to claim 13 performing processing generated as right-of-use information which stored right permit information of contents playback based on a preset value of an audition flag set as a contents file in default right-of-use information.
[Claim 15]
It is the computer program which described decoding and a regeneration execution program of enciphered content
A step which judges whether it is regeneration of purchase contentsor it is audition processing of contents
A reproduction propriety decision processing step based on description of right-

of-use information corresponding to contents which perform as conditions that it is regeneration of purchase contents
A reproduction propriety decision processing step based on description of default right-of-use information as contents right-of-use information corresponding to audition processing which performs as conditions that it is audition processing of contents
A ****(ing) computer program.
[Claim 16]
It is the computer program which described an information processing execution program in a license server which publishes contents right-of-use information over a client which performs contents playback
A step which receives a registry request from a client
Service information which stored validation key blocks (EKB) which contain a device node key (DNK) which is needed in the case of decoding processing of enciphered content according to reception of said registry requestA step which generates default right-of-use information as contents right-of-use information applied to a reproduction propriety judging in audition processing of contents in a client
A step which transmits generated service information and default right-of-use information to a client
A ****(ing) computer program.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]
This invention relates to an information processoran information processing methodand a computer program. It is related with the information processor which realized the check of the contents right of use in utilization timesuch as reproduction of contentsand enabled audition of contentsand preview processing and realized the flexible contents use mode to a user especiallyan information processing methodand a computer program.
[0002]
[Description of the Prior Art]
Various software datasuch as these daysmusic dataa game programand image data. Circulation through the storage of networks of (calling these the contents (Content) hereafter)such as the Internetor a memory cardHDDVDCDetc. which can be circulated prospers. These circulation contents are stored in the memory measure in PC (PersonalComputer) which a user ownsa record reproducerthe vessel only for playbackor a game machine machinefor exampleHDthe card type storage which has a flash memoryCDDVDetc.and regeneration is performed.
[0003]

To information machines and equipmentsuch as a recording and reproducing devicea game machine machineand PC. The interface for receiving contents from a networkor a memory cardIt has an interface for accessing HDDVDCDetc.and has RAMROMetc. which are used as a memory area of the control means which is needed for playback of contentsa programand data.
[0004]
Various contentssuch as music dataimage dataor a programWith directions of the user through the input means which was user-directed or was connected from main parts of information machines and equipmentsuch as the recording and reproducing device and game machine machine which are used as playback apparatusand PC. For exampleit is called from built-in or the storage which can be detached and attachedand is reproduced through the main part of information machines and equipment or the connected displaya loudspeakeretc.
[0005]
As for many software contentssuch as a game programmusic dataand image datathe right of distributionetc. are generally held by the maker and the vender. Thereforeit is common to license softwareand for reproduction without permissionetc. to be made not to be performednamelyto take the composition in consideration of security only to fixed use restrictionsi.e.a regular userwhen distributing these contents.
[0006]
Contents and the right of use using contents are managed independentlyand the composition with which a user is provided is proposed. By acquiring the contents encipheredfor example and purchasing right-of-use data furtherbased on key data acquirable from right-of-use data etc.a user acquires the key for decoding of enciphered content (contents key)and uses contents in this composition.
[0007]
The setup information of a user's contents utilization permission mode is stored in right-of-use dataand the system that use of the contents in the range allowed in the permit information is attained is proposed.
[0008]
[Problem(s) to be Solved by the Invention]
Thuscontents and the contents right of use are managed independentlyand the check of right-of-use data is performed in the system with which a user is provided on the occasion of reproduction of use of contentsfor examplemusic dataand image datadistributionor download processing.
[0009]
In such compositionwhen judged with there being no right for a user to use contentsin the case of a right-of-use checkreproduction of contentsdistributionand download will be performed.
[0010]
Howeverafter performing the audition or the preview for some contents and checking the contents of contents before the purchase of contentsIt is also a fact that there is a request of liking to purchase contentsand if check processing of

the usual contents right of use is performed in such a caseprocessing of contents playback etc. will be refused by judgment that there is no right of use.
[0011]
In order to correspond to such a situationit is also possible to have composition which distributes the free sample data which does not take the right of use into consideration at all to a userbut an author's copyright and a distributor's right of distribution exist in almost all contents. Thereforeeven if it is some contentsthe situation where contents circulate disorderly and a copy is performed without notice among users is not a desirable thing.
[0012]
The purpose of this invention is as follows.
Be made in view of such a situationand a user needs to perform regular purchase processing of contents and enable just contents use based on the right of use. Provide the information processor which made it possible to perform the contents audition without purchase for contentsor a previewan information processing methodand a computer program.

[0013]
An object of this invention is to provide the information processor which enabled prevention of disorderly secondary circulation of audition data and preview data furtheran information processing methodand a computer program.
[0014]
[Means for Solving the Problem]
The 1st side of this invention
It is an information processor which performs decoding of enciphered contentand regeneration
As contents playback conditionsit has a control means which performs regeneration based on this contents right-of-use information with reference to contents right-of-use information
Said control means
When reproducing purchase contentsa reproduction propriety judging based on description of right-of-use information corresponding to contents is performed
It is in an information processor having the composition which performs a reproduction propriety judging based on description of default right-of-use information as contents right-of-use information corresponding to audition processing on the occasion of audition processing of contents.
[0015]
An information processor of this invention sets like 1 operative conditionand said default right-of-use informationHave right permit information of contents playback based on a preset value of an audition flag set as a contents fileand said control meansOn the occasion of audition processing of contentsan audition flag added to contents for an audition is verifiedand it is characterized by being the composition of judging reproductive propriety based on this verification result.
[0016]

An information processor of this invention sets like 1 operative conditionand said information processorStore purchase reproduction execution application applied to purchase regeneration of contentsand audition processing execution application applied to audition processing of contentsand said control meansIt is characterized by being the composition of choosing and performing either said purchase reproduction execution application or audition processing execution application based on a startup file to input from the outside.

[0017]

An information processor of this invention sets like 1 operative conditionand said information processorStore purchase reproduction execution application applied to purchase regeneration of contentsand audition processing execution application applied to audition processing of contentsand said control meansIt is characterized by being the composition of choosing and performing either said purchase reproduction execution application or audition processing execution application based on an extension set as a startup file to input from the outside.

[0018]

An information processor of this invention sets like 1 operative conditionand said enciphered contentAre the contents enciphered by the contents key Kc and said contents key KcIt is a key acquirable only by application of a key acquirable by decoding of validation key blocks (EKB) provided with the application of validation key-blocks (EKB) distribution tree compositionSaid control means is characterized by being the composition of performing contents key acquisition processing by decoding processing of said validation key blocks (EKB).

[0019]

The 2nd side of this invention

It is an information processor as a license server which publishes contents right-of-use information over a client which performs contents playback

Service information which stored validation key blocks (EKB) which contain a device node key (DNK) which is needed in the case of decoding processing of enciphered content according to a registry request from a client

Default right-of-use information as contents right-of-use information applied to a reproduction propriety judging in audition processing of contents in a client is generatedand it is in an information processor having the composition which performs processing published to a client.

[0020]

An information processor of this invention sets like 1 operative conditionand said information processor has the composition which performs processing which generates default right-of-use information that right permit information of contents playback based on a preset value of an audition flag set as a contents file was stored.

[0021]

The 3rd side of this invention

It is an information processing method which performs decoding of enciphered contentand regeneration

As contents playback conditionsit has a contents playback control step which performs regeneration based on this contents right-of-use information with reference to contents right-of-use information
Said contents playback control step is further
A step which judges whether it is regeneration of purchase contentsor it is audition processing of contents
A reproduction propriety decision processing step based on description of right-of-use information corresponding to contents which perform as conditions that it is regeneration of purchase contents
It is in an information processing method containing a reproduction propriety decision processing step based on description of default right-of-use information as contents right-of-use information corresponding to audition processing which performs as conditions that it is audition processing of contents.
[0022]
An information processing method of this invention sets like 1 operative conditionand said default right-of-use informationHave right permit information of contents playback based on a preset value of an audition flag set as a contents fileand said contents playback control stepOn the occasion of audition processing of contentsan audition flag added to contents for an audition is verifiedand reproductive propriety is judged based on this verification result.
[0023]
An information processing method of this invention sets like 1 operative conditionand said information processing methodBased on a startup file to inputfrom the outsidepurchase reproduction execution applicationOr it has a selection step which chooses either of the audition processing execution applicationsand said contents playback control step is performed according to AUPURIKESHON selected in said selection step.
[0024]
An information processing method of this invention sets like 1 operative conditionand said information processing methodA step which distinguishes an extension of a startup file inputted from the outsideBased on an extension of a distinguished startup filepurchase reproduction execution applicationOr it has a selection step which chooses either of the audition processing execution applicationsand said contents playback control step is performed according to AUPURIKESHON selected in said selection step.
[0025]
An information processing method of this invention sets like 1 operative conditionand said enciphered contentAre the contents enciphered by the contents key Kc and said contents key KcIt is a key acquirable only by application of a key acquirable by decoding of validation key blocks (EKB) provided with the application of validation key-blocks (EKB) distribution tree compositionSaid contents playback control step contains a step which performs contents key acquisition processing by decoding processing of said validation key blocks (EKB).
[0026]

The 4th side of this invention
It is an information processing method in a license server which publishes contents right-of-use information over a client which performs contents playback
A step which receives a registry request from a client
Service information which stored validation key blocks (EKB) which contain a device node key (DNK) which is needed in the case of decoding processing of enciphered content according to reception of said registry requestA step which generates default right-of-use information as contents right-of-use information applied to a reproduction propriety judging in audition processing of contents in a client
A step which transmits generated service information and default right-of-use information to a client
It is in a ****(ing) information processing method.
[0027]
An information processing method of this invention sets like 1 operative conditionand processing generated as right-of-use information which stored right permit information of contents playback based on a preset value of an audition flag set as a contents file in default right-of-use information is performed in said information processing method.
[0028]
The 5th side of this invention
It is the computer program which described decoding and a regeneration execution program of enciphered content
A step which judges whether it is regeneration of purchase contentsor it is audition processing of contents
A reproduction propriety decision processing step based on description of right-of-use information corresponding to contents which perform as conditions that it is regeneration of purchase contents
A reproduction propriety decision processing step based on description of default right-of-use information as contents right-of-use information corresponding to audition processing which performs as conditions that it is audition processing of contents
It is in a ****(ing) computer program.
[0029]
The 6th side of this invention
It is the computer program which described an information processing execution program in a license server which publishes contents right-of-use information over a client which performs contents playback
A step which receives a registry request from a client
Service information which stored validation key blocks (EKB) which contain a device node key (DNK) which is needed in the case of decoding processing of enciphered content according to reception of said registry requestA step which generates default right-of-use information as contents right-of-use information applied to a reproduction propriety judging in audition processing of contents in a

client
A step which transmits generated service information and default right-of-use information to a client
It is in a ****(ing) computer program.
[0030]
[Function]
According to the composition of this inventiona client acquires default right-of-use information (Default Usage Right) in the case of the registration processing to a license serverBased on default right-of-use informationcontents playback is permitted in the case of the audition processing without purchase processing of contentsand the audition reproduction of contents of a user is attainedwithout performing the purchase of contents. The client to which an audition is permitted performs registration processing to a license serverand since it will be limited to the client which has default right-of-use informationaudition data is prevented from overflowing disorderly.
[0031]
Also in the audition processing without [according to the composition of this invention] purchase processing of contentsThe hard correspondence EKB as EKB corresponding to the category tree set up corresponding to the hardware as contents use apparatus [EKB (H)]The composition whose execution of contents playback only the user who has just DNK to the service correspondence EKB as EKB corresponding to the category tree set up corresponding to contents use service [EKB (S)] enables is applicableSetting out becomes possible as a range which limited reproduction authority also in audition processing.
[0032]
The computer program of this inventionFor examplethe general purpose computer system which can execute various program codes is receivedIt is a computer program which can be provided by communication mediasuch as storagessuch as a storage provided in a computer-readable formcommunication mediafor exampleCDFDMOor a network. By providing such a program in a computer-readable formprocessing according to a program is realized on computer systems.
[0033]
The purposethe featureand advantage of further others of this invention will become clear [rather than] by detailed explanation based on the example and the drawing to attach of this invention mentioned later. In this specificationa system is the logical set composition of two or more devicesand it does not restrict to what has a device of each composition in the same case.
[0034]
[Embodiment of the Invention]
Hereafterthe composition of this invention is explained in detail. Explanation is performed according to each item shown below.
1. Contents providing system outline
2. About the tree (Thurs.) structure as key distribution composition
3. Distribution of key which uses EKB

4. Format of EKB
5. Categorization of tree
6. Content purchase and audition processing
7. Backup/restoration processing
8. Secondary distribution of contents by recommendation file

[0035]

[1. Contents providing system outline]

Drawing 1 is a figure explaining the outline of the contents providing system which applied this invention. The client 10 using contents is an information processor as usei.e.refreshable apparatusabout contents. For examplevarious kinds of information processorssuch as PC and PDAare contained. The client 10 has the browser 11 and the client application 12 as softwareand a program besides the browser 11 and the client application 12 is executed by control meanssuch as CPU.

[0036]

The purchase of contents and audition processing[in / in the client application 12 / a client] The acquisition processing of the service information explained in the latter partand license information including contents right-of-use informationIt is the application which performs contents and backup/restoration processing of license informationconfirming processing of the contents right of usecontents playback management processingor generation processing of the recommendation file as a contents file for secondary distribution.

Hereafterit is stored in the information processor of a client as a processing program explained in detail.

In this specificationa "audition" is used as a meaning which includes not only the audition of voice data but the preview of image data.

[0037]

The client 10 is connected with the shop server 21the license server 22and the contents server 23for example via communications networkssuch as the Internet. The contents server 23 provides contents to the client 10. The license server 22 provides the right-of-use information on the contents which a client uses to the client 10. The shop server 21 functions as a window at the time of the client 10 purchasing contentspresents the contents listening can be tried [purchase or] via a browserand receives the demand of the purchase from a clientor an audition. Accounting about purchase contents is performed if needed.

[0038]

The managerial system 31 is connected to the shop server 21 and the license server 22. The managerial system 31 performs issue processing of transaction ID (TID) which functions as permit information over the contents request from the client 10 which the shop server 21 receivedand issue processing of contents download permit information. The managerial system 31 performs the issuing permission of the right-of-use data Usage Right as right-of-use information on contents to the license server 22. The latter part explains the details of these processings.

[0039]
The client 10 Acquisition of the right of use from the license server 22Performing the contents acquisition from the contents server 23 under control of the client application 12the inspection and settlement processing of information which the shop server 21 provides start and perform the browser 11 under control of the client application 12.
[0040]
Although a client and each one server of every are shown in drawing 1Much these are connected on communications networkssuch as the Internetand a clientConnect with various shop servers and the contents provided by each shop server are chosen freelyThe license server which publishes the right of use of the contents which acquired contents and were acquired from the contents server which stored selected contents is chosenand the right of use is acquired from the selected license server.
[0041]
The client 10 is provided with contents from the contents server 23 as enciphered content. The client 10 is received from the license server 22The contents right-of-use information corresponding to contents is providedand right-of-use information is verifiedand when the client application 12 of the client 10 is judged as there being the right of useit decodes and uses enciphered content.
[0042]
The client 10 holds key datasuch as validation key blocks (EKB:Enabling Key Block) and a device node key (DNK:Device Node Key)as key information for enabling contents use based on the contents right of use. Validation key blocks (EKB:Enabling Key Block) and a device node key (DNK:Device Node Key)It is key data for acquiring the encryption key which is needed for the contents use for decoding enciphered content only in the user device which has the just contents right of use for use of contentsand supposing that it is available. The latter part explains EKB and DNK.
[0043]
The contents server 23 enciphers contents and provides the client 10 with enciphered content. The license server 22 generates right-of-use information (Usage Right) based on a contents utilization conditionand provides the user device 30 with it. Service information is generated based on the device node key (DNK:Device Node Key) and validation key blocks (EKB:Enabling Key Block) which the managerial system 31 providesand it provides for the client 10. Service information contains validation key blocks (EKB) with the service device node key (SDNK) which is needed in the case of the decoding processing of enciphered content.
[0044]
The utilization conditions of contents include the limiting conditions of an available termnumber-of-times restrictions of a copya number (it corresponds to what is called the number of check-out (Check-out)) of portable media (PM:Portable Media) of restrictions that can use contents simultaneously furtheretc. Portable

media (PM:Portable Media) are available storages in portable devicessuch as a flash memory or small HDan optical disca magneto-optical discand MD (Mini Disk).
[0045]
Nextwith reference to drawing 2the example of composition of the information processor in which a function is possible as the client 10the shop server 21the license server 22the contents server 23and the managerial system 31 is shown. For exampleeach of these systems have CPUthey are realized by storing the processing program according to each processing in systemssuch as PC and a server.
[0046]
Firstthe example of composition of each system is explained using drawing 2. Various programs CPU(Central Processing Unit) 101 are remembered to be by ROM(Read Only Memory) 102Or it is stored in the storage parts store 108and various processing is performed according to the program loaded to RAM(Random Access Memory) 103. the timer 100 -- a time check -- it processes and clock information is supplied to CPU101.
[0047]
ROM(Read Only Memory) 102 stores a parameter for a program or an operationfixed dataetc. which CPU101 uses. In the program used in execution of CPU101and its executionRAM(Random Access Memory) 103 stores a variable parameter etc. suitably. These each element is mutually connected by bus 111 which comprises a CPU bus etc.
[0048]
The encryption decoding part 104 as application processing of encryption of contentsdecoding processinga device node key (DNK:Device Node Key)and validation key blocks (EKB:Enabling Key Block)For examplecipher processingMAC generationverification processingetc. which applied the encryption algorithm of DES (Data Encryption Standard) are performed. Various cipher processingsuch as attestation at the time of transmission and reception of the contents or license information performed among other contacts and session key share processingis performed.
[0049]
The codec part 105 performs data encoding processing of various methodssuch as ATRAC(Adaptive Transform Acoustic Coding)3 methodMPEGa JPEG systemand decodingfor example. Processing-object data is inputted via the communications department 109 via the bus 111the input/output interface 112and the drive 110 from the removable storage medium 121. The data after processing is stored in the removable storage medium 121 if neededor is outputted via the communications department 109.
[0050]
In the input/output interface 112the input parts 106such as a keyboard and a mouseCRTData transmission and reception which the communications department 109 constituted by the storage parts stores 108such as the outputting part 107 and a hard diska modema terminal adopteretc. which consist of a display of LCD

etc.a loudspeakeretc. was connectedfor examplepassed communications networkssuch as the Internetis performed.
[0051]
[-- 2. -- the tree (Thurs.) structure as key distribution composition --]
Nextthe management composition of a device and a key by the tree composition which is one mode of a broadcasting encryption (Broadcast Encryption) method for making contents available only in the client which has the just contents right of use is explained.
[0052]
The numbers 0-15 shown in the bottom of drawing 3 are the user devices as a client which performs contents use. That iseach leaf (leaf: leaf) of the hierarchy tree (Thurs.) structure shown in drawing 3 is equivalent to each device.
[0053]
each devices 0-15 -- the time of manufacture or shipment -- or it setting after that andThe key set (device node key (DNK:Device Node Key)) which consists of a key (node key) assigned to the node of a to [from its own leaf in the hierarchy tree (Thurs.) structure shown in drawing 3 / a route] and a leaf key of each leaf is stored in a memory. K0000-K1111 which are shown in the bottom of drawing 3 are the leaf key assigned to each devices 0-15respectivelyand let key:KR-K111 indicated in the 2nd paragraph (node) from the bottom be a node key from KR (route key) of the highest rung.
[0054]
In the tree composition shown in drawing 3the device 0 owns the leaf key K0000node key:K000 and K00K0and KR. The device 5K0101K010K01K0and KR are owned. The device 15 owns K1111K111K11K1and KR. Although 16 devices of 0-15 are indicated to the tree of drawing 3 and the tree structure is also shown as symmetrical composition which was able to take balance of 4 stage constitutionit is possible to have number-of-stages composition which much more devices are constituted in a treeand is different in each part of a tree.
[0055]
The device various type which uses DVDCD and MD which were constituted by various recording mediafor examplea device embedding typeor the device enabling free attachment and detachmenta flash memoryetc. is contained in each device contained in the tree structure of drawing 3. Various application services can live together. The hierarchy tree structure which is the contents or the key distribution configuration shown in drawing 3 after such a different device and different application constitute [coexistence] is applied.
[0056]
In the system by which these various devices and application live togetherthe portion 012and 3 enclosed with the dotted line of drawing 3i.e.devicesis set up as one group using the same recording medium. For examplethe device contained in the group enclosed with this dotted line is receivedIt collectsand common contents are enciphered and processing in which send the contents key which is sent from a provider or is used [each device]or encipher to a provider or a

settlement-of-accounts organization tooand the payment data of a content rate is outputted to it from each device is performed. Processing which a contents servera license serveror a shop server bundles up the portion 012and 3 surrounding [with the dotted line of drawing 3] the organization which performs data transmission and reception with each devicei.e.devicesas one groupand sends data is performed. Two or more such groups exist in the tree of drawing 3. The organization which performs data transmission and reception with each devicessuch as a contents servera license serveror a shop serverfunctions as a message data distribution means.

[0057]

May generalize and manage a node key and a leaf key with a managerial system with one certain lock management center functionandIt is good also as composition managed for every group by message data distribution meanssuch as a provider who performs various data transmission and reception to each groupand a settlement-of-accounts organization. As for these node keys and a leaf keyin disclosure of a keyetc.an update process is performedand a managerial systema providera settlement-of-accounts organizationetc. with a lock management center function perform this update process.

[0058]

In this tree structureso that clearly from drawing 3The three devices 012and 3 contained in one group hold the key K00 common as a device node key (DNK:Device Node Key)K0and the device node key (DNK:Device Node Key) containing KR. By using this node key share compositionit becomes possible to provide only the devices 012and 3 with a common keyfor example. For examplethe node key K00 held in common turns into a possession key common to the devices 012and 3. If the value Enc (K00Knew) which enciphered the new key Knew by the node key K00 is stored in a recording medium via a network and distributed to the devices 012and 3Only the devices 012and 3 become possible [solving the code Enc (K00 Knew) using the share node key K00 held in each deviceand obtaining the new key Knew]. It is shown that Enc (KaKb) is the data which enciphered Kb by Ka.

[0059]

When it is revealed in t at a certain time that key:K0011 which the device 3 ownsK001K00K0and KR were analyzed by the aggressor (hacker)and it was exposed of KRAfter itin order to protect the data transmitted and received by a system (group of the devices 012and 3)it is necessary to separate the device 3 from a system. for that purpose -- a node key -- : -- K -- 001 -- K -- 00 -- K -- zero -- KR -- respectively -- being new -- a key -- K -- (-- t --) -- 001 -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- updating -- a device -- zero -- one -- two -- the -- updating -- a key -- it is necessary to tell . Hereit is shown that K(t) aaa is an updating key of generation (Generation):t of the key Kaaa.

[0060]

distribution **** of an updating key -- it ****** just. The renewal of a key the

table constituted by the block data called the validation key blocks (EKB:Enabling Key Block) shown in drawing 4 (A)for example For examplea networkOr it performs by storing in a recording medium and supplying the devices 01and 2. Validation key blocks (EKB) are constituted by the cryptographic key for distributing the key newly updated by the device corresponding to each leaf which constitutes a tree structure as shown in drawing 3. Validation key blocks (EKB) may be called the renewal block of a key (KRB:Key Renewal Block).

[0061]

It is constituted as block data which has a data configuration which can update only the required device of renewal of a node key in the validation key blocks (EKB) shown in drawing 4 (A). In the devices 01and 2 in the tree structure shown in drawing 3the example of drawing 4 is the block data formed for the purpose of distributing the generation's t updating node key. drawing 3 -- from -- being clear -- as -- a device -- zero -- a device -- one -- updating -- a node key -- ****** -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- required -- a device -- two -- updating -- a node key -- ****** -- K -- (-- t --) -- 001 -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- being required .

[0062]

As shown in EKB of drawing 4 (A)two or more cryptographic keys are contained in EKB. The cryptographic key of the bottom is Enc (K0010K(t)001). this -- a device -- two -- having -- a leaf key -- K -- 0010 -- enciphering -- having had -- updating -- a node key -- K -- (-- t --) -- 001 -- it is -- a device -- two -- self -- having -- a leaf key -- this -- a cryptographic key -- decoding -- K -- (-- t --) -- 001 -- it can obtain . using K(t)001 obtained by decodingdecoding of the 2nd step of cryptographic key Enc (K -- (-- t --) -- 001 -- K -- (-- t --) -- 00) is attained from under drawing 4 (A)and updating node key K(t)00 can be obtained. belowone by onethe 2nd step of cryptographic key Enc (K -- (-- t --) -- 00 -- K -- (-- t --) -- 0) is decoded from on drawing 4 (A)the 1st step of cryptographic key Enc (K(t) 0 and K (t) R) is decoded from on updating node key K(t)0 and drawing 4 (A)and K(t) R is obtained. on the other hand -- a device -- K -- 0000 . -- K -- 0001 -- a node key -- K -- 000 -- updating -- an object -- containing -- not having -- updating -- a node key -- ****** -- being required -- a thing -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- it is . Device K0000.K0001 decodes the 3rd step of cryptographic key Enc (K000K(t)00) from on drawing 4 (A)and acquires K(t)00hereafterthe 2nd step of cryptographic key Enc (K -- (-- t --) -- 00 -- K -- (-- t --) -- 0) is decoded from on drawing 4 (A)the 1st step of cryptographic key Enc (K(t) 0 and K (t) R) is decoded from on updating node key K(t)0 and drawing 4 (A)and K(t) R is obtained. Thusthe devices 01and 2 can obtain updated key K(t) R. The index of drawing 4 (A) shows the actual address of the node key and leaf key which are used as a decryption key.

[0063]

The node key of the upper stage of the tree structure shown in drawing 3 : when renewal of K(t) 0 and K (t) R is unnecessary and the update process of only the

node key K00 is requiredBy using the validation key blocks (EKB) of drawing 4 (B)updating node key K(t)00 can be distributed to the devices 01and 2.
[0064]
EKB shown in drawing 4 (B) is available when distributing the new contents key sharedfor example in a specific group. As an examplethe recording medium with the devices 012and 3 in the group who shows by a dotted line is used for drawing 3and suppose that new common contents key K(t) con is required. this -- the time -- a device -- zero -- one -- two -- three -- being common -- a node key -- K -- 00 -- having updated -- K -- (-- t --) -- 00 -- using -- being new -- being common -- updating -- a contents key -- : -- K -- (-- t --) -- con -- having enciphered -- data -- Enc (K(t) K(t) con) -- drawing 4 -- (-- B --) -- being shown -- EKB -- distributing . By this distributionthe distribution as data of the device 4 etc. which is not decoded in other groups' apparatus is attained.
[0065]
That isif the devices 01and 2 decode the above-mentioned cryptogram using K(t)00 which processed and obtained EKBit will become possible to obtain contents key K(t) con applied to the key in t timefor exampleencryption decryption of contents.
[0066]
[3. Distribution] of the key which uses EKB
As an example of processing which obtains contents key K(t) con applied to the key in t timefor exampleencryption decryption of contentsat drawing 5K (t) The example of processing of the device 0 which received EKB shown in the data Enc (K (t) 00K(t) con) which enciphered new common contents key K(t) con using 00and drawing 4 (B) via the recording medium is shown. That isit is the example which set the encryption message data based on EKB to contents key K(t) con.
[0067]
As shown in drawing 5the device 0 generates node key K(t)00 by same EKB processing with having mentioned above using the node key K000 which EKB and the them at the generation:t time stored in the recording medium store beforehand. Updating contents key K(t) con is decoded using updating node key K(t)00 decodedand in order to use it behindit enciphers and stores by the leaf key K0000 which he has.
[0068]
[4. Format] of EKB
The example of a format of validation key blocks (EKB) is shown in drawing 6. The version 201 is an identifier which shows the version of validation key blocks (EKB). A version has a function which shows the correspondence relation of the function and contents which identify the newest EKB. A depth shows the hierarchy number of the hierarchy tree to the device of the distribution destination of validation key blocks (EKB). The data pointer 203 is a pointer in which the position of the data division in validation key blocks (EKB) is shown.
It is a pointer which the tag pointer 204 shows the position of a tag part toand the signature pointer 205 shows the position of a signature.

[0069]
The data division 206 stores the data which enciphered the node key updatedfor example. For exampleeach cryptographic key about the updated node key as shown in drawing 5 is stored.
[0070]
The tag part 207 is a tag in which the physical relationship of the node key and leaf key which were stored in the data divisionand which were enciphered is shown. The grant rule of this tag is explained using drawing 7. Drawing 7 shows the example which sends the validation key blocks (EKB) previously explained by drawing 4 (A) as data. The data at this time comes to be shown in the table (b) of drawing 7. Let the address of the top node contained in the cryptographic key at this time be a top node address. In this casesince updating key K(t) R of the route key is containeda top node address serves as KR. At this timethe data Enc (K(t) 0 and K (t) R) of the highest rung is in the position shown in the hierarchy tree shown in (a) of drawing 7for example. Herethe following data is Enc (K (t) 00K(t)0). It is in the position at the lower left of front data on a tree.
A tag is set upand 1 is set up when there is dataand there is nothing0 and. A tag is set up as {a left (L) tag and a right (R) tag}. Since there is data in the left of the data Enc (K(t) 0 and K (t) R) of the highest rung and there is no data in L tag =0 and the rightit is set to R tag =1. Hereaftera tag is set as all the data and the data row shown in drawing 7 (c) and a tag sequence are constituted.
[0071]
A tag is set up in order to show where [of a tree structure] the data Enc (KxxxKyyy) is located. the key data Enc (KxxxKyyy) stored in a data division -- since ... is only enumeration data of the key enciphered simplyit enables distinction of the position on the tree of the cryptographic key stored as data with the tag mentioned above. using the node index to which encryption data was made to correspond like composition of that previous drawing 4 explainedwithout using the tag mentioned above -- for example
0:Enc(K(t)0K(t)root)
00:Enc(K(t)00K(t)0
000:Enc(K((t)000K(T)00)
Although it is also possible to consider it as a data configuration like ...in the distribution etc. which it will become redundant data and data volume will increase if it has composition using such an indexand pass a networkit is not desirable. On the other handdistinction of a key position is attained with small data volume by using the tag mentioned above as index data in which a key position is shown.
[0072]
It returns to drawing 6 and an EKB format is explained further. For examplethe signature (Signature) 208 published validation key blocks (EKB)it is an electronic signature which a managerial system and a contents server with a lock management center functiona license serveror a shop server performs. It checks that the devices which received EKB are the validation key blocks (EKB) which the

just validation key-blocks (EKB) publisher published by signature verification.
[0073]
[5. Categorization] of a tree
The composition which classifies the hierarchy tree structure which defines the node key etc. for every category of each deviceand performs an efficient key update processcryptographic key distributionand data distribution is explained below.
[0074]
An example of a classification of the category of a hierarchy tree structure is shown in drawing 8. In drawing 8route key Kroot301 is set to the highest rung of a hierarchy tree structurethe node key 302 is set to the following intermediate stagesand the leaf key 303 is set to the bottom. Each device holds each leaf keyand a series of node keys from a leaf key to a route key and a route key.
[0075]
Herethe existing node of the Mth step is set up as the category node 304 from the highest rung as an example. That islet each of the node of the Mth step be a device setting-out node of a specific category. Let M+1 or less step of nodeand a leaf be the node and leaf about the device contained in the category hereafter by making one node of the Mth step into the peak.
[0076]
For examplea category [memo RISUTEIIKU (trademark)] is set to the one node 305 of the Mth step of drawing 8and the node which stands in a row below in this nodeand a leaf are set up as the node or leaf only for a category containing various devices which use memo RISUTEIIKU. That is305 or less node is defined as the related node of the device defined as the category of a memory stickand a set of a leaf.
[0077]
The low-ranking stage can be set up as the subcategory node 306 by several steps from M stage. For examplethe node of [the vessel only for reproduction] is set up as a subcategory node contained in the category of the device which uses a memory stick for the node under two steps of the category [memory stick] node 305 as shown in a figure. To 306 or less node of the vessel only for reproduction which is a subcategory node. The node 307 of the telephone with a music reproduction function included in the category of the vessel only for playback is set upand the [PHS] node 308 and the [cellular-phone] node 309 which are contained in the low rank at the category of a telephone with a music reproduction function can be set up further.
[0078]
A category and a subcategory only not only in the kind of devicefor example A certain makerIt is possible to set up in arbitrary units (these are generically called an entity hereafter)such as the node which a content providera settlement-of-accounts organizationetc. manage uniquelyi.e.a batcha jurisdiction unitor a providing service unit. For exampleif one category node is set up as a peak node only for game machine machine XYZ which a game machine machine maker sellsIn

the game machine machine XYZ which a maker sellsthe node key of the lower berth below the peak nodeStorebecome a leaf key possible to sell and Distribution of after that and enciphered contentOr the validation key blocks (EKB) constituted by the node key below the peak node key and the leaf key in distribution of various keys and an update process are generated and distributedand distribution of available data is attained only to the device below a peak node.

[0079]

Thusby considering the following nodes as the category defined as the peak nodeor the composition set up as a related node of a subcategory by making one node into the peakThe maker which manages one peak node of the category stage or the subcategory stagea content provideretc. generate uniquely the validation key blocks (EKB) which make the node the peakThe composition distributed to the device belonging to below a peak node is attainedand renewal of a key can be performedwithout affecting at all the device belonging to the node of other categories which do not belong to a peak node.

[0080]

In the system of this inventionas shown in drawing 9it is a system of tree composition and key management is performed. In the example of drawing 98+24+32 steps of nodes are made into a tree structureand a category corresponds to each node from a root node to eight steps of a low rank. The category in here means categoriessuch as a category of the apparatus which uses semiconductor memorysuch as a memory stickfor exampleand a category of apparatus which receives digital broadcasting. And this system (T system is called) corresponds to one node in this category node as a system which manages a license.

[0081]

That isthe key corresponding to 24 steps of a younger hierarchy's nodes is further applied to the service which a service provider or a service provider provides from the node of this T system. In the case of this exampletherebythe service provider of 2^{24} (about 16 mega) or service can be specified. 32 steps of lower hierarchies can prescribe the user (or user device) of 2^{32} (about 4 giga). The key corresponding to each node on the path from 32 steps of nodes of the bottom to the node of T system constitutes DNK (DeviceNode Key)and ID corresponding to the leaf of the bottom is set to leaf ID.

[0082]

For examplethe contents key which enciphered contents is enciphered by updated route key KR'it is enciphered using the updating node key of the hierarchy of the latest low rankand the updating node key of the hierarchy of a higher rank is arranged in EKB. The updating node key of the stage on one is enciphered from the end in EKB by the node key or leaf key of an end of EKBand it is arranged in EKB.

[0083]

One key of the DNK(s) described by service information is used for a user deviceUsing the key which decoded the updating node key of the hierarchy of the

latest higher rank described in EKB distributedand decoded and obtained it with contents datafurthermore it is described in EKBthe updating node key of the hierarchy on it is decoded. By performing the above processing one by onethe user device can obtain updating route key KR'.
[0084]
As mentioned aboveone node is made into the peak by the categorization of a treeThe composition which set up the following nodes as the category defined as the peak node or a related node of a subcategory is attainedThe maker which manages one peak node of the category stage or the subcategory stagea service provideretc. generate uniquely the validation key blocks (EKB) which make the node the peakand composition distributed to the device belonging to below a peak node is realized.
[0085]
The EKB distribution system by device management of above-mentioned tree composition is appliedand the contents distribution and the usage pattern which adopted the EKB distribution composition based on two or more categories are explained.
[0086]
Two categories are explained with reference to drawing 10. As shown in drawing 10T system node 351 is set as the lower berth of the root node 350and the T service node 352 and the T hard node 353 are set as the lower berth. The tree which made the T hard node 353 the peak is a category tree which distributes the hard correspondence EKB [EKB (H)] which sets up user device apparatus itself as the leaf 355and is published for apparatus. On the other handthe tree which made the T service node 352 the peak is a category tree which distributes the service correspondence EKB [EKB (S)] which publishes corresponding to the service which provides for user device apparatus.
[0087]
The hard correspondence EKB [EKB (H)] and the service correspondence EKB [EKB (S)]having a key corresponding to each node on DNK (Device Node Key)i.e.the path from a leaf to the node of T systemgiven to a device with respectively just authority -- every -- decoding of EKB is attained.
[0088]
[6. Content purchase and audition processing]
Nextthe details of the processing at the time of a client purchasing or trying listening contents are explained below with reference to drawing 11.
[0089]
Drawing 11 shows the initial step of the communication sequence in the content purchase processing performed between clients which have client application and a browsersuch as PCand a shop servera contents servera license server and a managerial system. Hereafterthe processing shown in a sequence diagram is explained.
[0090]
Firstthe user who tries to purchase contents in a client sideThe contents list

screen (shop page) which specifies URL as the information processor of self PC etc. which can be communicated (step (1))a browser passesand a shop server presents is read (step (2))and it displays on ** and a display (step (3)).
[0091]
a client chooses contents from the contents list which a shop server presents -- further -- purchase or an audition -- one of specification (step (4)) is performed and requested data is transmitted to a shop server via a browser (step (5)). requested data -- content ID (CID)a shop server identifier (ShopID) and purchaseor an audition -- one of tbe data are contained.
[0092]
A shop server will require the propriety judging of offer of contents from a managerial systemif the content purchase from a client or an audition demand is received (step (6)). Content ID (CID) and a shop server identifier (ShopID) are contained in this judgment demand.
[0093]
A managerial system will perform issue processing (step (7)) of transaction ID (TID)if the propriety judging demand of offer of contents is received. The details of the issue processing of transaction ID (TID) are explained with reference to the flow of drawing 12.
[0094]
Firstin Step S101a managerial system generates a random number and generates transaction ID (TID) based on a generating random number. Nextin Step S102generated transaction ID (TID) and the content ID (CID) specified from the shop server are matchedand it stores in a storage parts store as transaction data. Nextgenerated transaction ID (TID) is outputted and published to a shop server.
[0095]
It returns to the sequence diagram of drawing 11. A managerial system transmits to a shop server after generation of transaction ID (TID) by making into TID information transaction ID (TID) and price information which were generated (step (8)). Howeverprice information is information demanded at the time of content purchase.
It is not contained on the occasion of contents audition processing.
The shop server which received TID information performs accounting (step (9)) based on the price contained in TID informationwhen the demand from a client is content purchase.
[0096]
When the demand from a client is not content purchase but a contents audition demandthis accounting (step (9)) is omitted.
[0097]
Nextthe processing continued with reference to the sequence diagram of drawing 13 is explained. In content purchase processing a shop serverOn condition that fee collection was performedin contents audition processingpurchase or the download permission demand of the contents for an audition demand is transmitted to a managerial system on condition of reception of the TID information from a

managerial system (step (10)).
[0098]
A managerial system will perform download permission demand verification processing (step (11))if a download permission demand is received. The details of download permission demand verification processing are explained with reference to the flow of drawing 14.
[0099]
Transaction ID (TID) contained in the download permission demand which received the managerial system in Step S201 firstFurther in [generate previouslycompare transaction ID (TID) stored in the storage parts storeand] Step S202The content ID (CID) recorded corresponding to transaction ID (TID) in which collation was materialized is acquiredand download permission of the contents corresponding to CID is published in Step S203.
[0100]
It returns to the sequence diagram of drawing 13and explanation is continued. A managerial system publishes download permission of contents to a shop server after download permission demand verification processing (step (11)) (step (12)). Transaction ID (TID)contents server URL (C-URL)license server URL (L-URL)content ID (CID)right-of-use information ID (UID)goods (contents) URL (S-URL)and service ID are contained in download permission.
[0101]
If download permission is received from a managerial systema shop serverThe startup file for starting the use programs (regeneration etc.) of the contents in client application is generatedand it sends to client application via the browser of a client.
[0102]
The example of a startup file is explained with reference to drawing 15. Transaction ID (TID) in which the managerial system generated the startup file 360 previouslyThe content ID (CID) which a client purchases or tries listeningright-of-use information ID (UID) contained in the download permit information which the managerial system generatedService ID contained in the download permit information which the managerial system generatedlicense server URLgoods (contents) URLand that identification data that processing is purchase or is auditions further are contained.
[0103]
As that identification data which processing is purchase or is an auditionthe extension set as a startup file is distinguished and set up by whether it is purchase or it is an auditionclient application distinguishes thisand it may be made to start each application.
[0104]
Client application starts application according to a startup file (step (15)).
[0105]
The application starting processing performed in client application is explained with reference to drawing 16. In Step S301it is judged whether the service information

corresponding to service ID set as the startup file is first stored in the information processor as a client system.

[0106]

Service information is data which accepts the right of service use which is received from a license server and the providing service of the specific service provider bundled upfor examplewhen a client wants to receivevarious kinds of servicesfor examplecontents use service. The example of a data configuration of service information is shown in drawing 17 (a).

[0107]

As shown in drawing 17 (a)to the service information 370. Leaf ID peculiar to the client set up in an EKB distribution treeservice ID as a service identifierthe data that enciphered the device node key (DNK) by the route key (Kroot) furtherand E (KrootDNK) are contained. In order to receive service informationregistration processing [as opposed to a license server in a client] is needed. Registration processing is equivalent to processing of the processing step (15) shown in drawing 13and (16).

[0108]

In Step S301 shown in drawing 16if it judges with not holding the service information corresponding to service IDregistration processing will be performed in Step S302and service information will be received.

[0109]

Default right-of-use information is published from a license server to a client at the time of this registration processing. Although right-of-use information stores the utilization condition of purchase contents and is usually published corresponding to the purchase of contentsDefault right-of-use information does not publish the purchase of contents as conditionsand publishes registration processing of a clientor issue processing of service information as conditions. This default right-of-use information is applied as effective contents right-of-use information in the case of audition processing of the contents explained in the latter part.

[0110]

The example of a data configuration of right-of-use information is shown in drawing 17 (b). As shown in drawing 17 (b)to the right-of-use information 371. When it is a time stamp as informationleaf ID peculiar to a clientand contents correspondence at the time of right-of-use information ID as a right-of-use information identifierand the date of issuethe contents type information for a utilization condition is stored in content ID and a pan.

[0111]

Since it is not what is published corresponding to specific purchase contents in the case of default right-of-use informationID with content ID common to the contents in which an abbreviation or an audition is possible is set up. It is considered as setting out to which the use about the contents to which the audition flag was set as the one (ON)for example is permitted as contents type information for a utilization condition. As shown in drawing 17 (c) at the contents

372the audition flag 373 is set upand if the audition flags 373 are setting-out contents of one (ON)It is shown that they are the contents to which the audition was permittedand if audition flags are setting-out contents of OFF (OFF)it is shown that they are contents to which the audition is not permitted.
[0112]
While client application judges the existence of a reproducing permission with reference to default right-of-use information at the time of audition contents playbackit will perform verification of the flag of contents and will reproduce contents. The latter part explains this processing.
[0113]
It returns to the process flow of drawing 16and the procedure of application starting processing is explained. In [after acquisition of registration processingi.e.the service information from a license serverand default right-of-use information is completed in Step S302] Step S303The startup file which received from the shop server distinguishes whether it is a startup file of the application for purchaseor it is a startup file of the application for an audition. When it is a startup file of the application for purchaseit progresses to Step S304 and application for purchase is performedwhen it is a startup file of the application for an auditionit progresses to Step S305 and application for an audition is performed.
[0114]
Nextthe execution sequence of the application for purchase is explained with reference to the sequence diagram of drawing 18.
[0115]
In purchase processing executionclient application performs a contents download request to a contents server (step (21)). This is the contents to which the client performed the purchase request previously.
They are the contents corresponding to the content ID (CID) recorded on right-of-use information (refer to drawing 17 (b)).
Client application specifies contents by content ID (CID)and performs a contents download request to a contents server.
[0116]
A contents server will transmit the contents information corresponding to CID to a clientif a contents download request is received (step (22)). Including enciphered contentas shown in drawing 17 (c)this contents informationContents key : Contents data:Enc enciphered by Kc (KcContent)contents key: -- Kc -- route key: -- they are EKB for acquiring data:Enc (KrootKc) enciphered by Krootand also :route key:Krootand the file to which informationincluding audition flag dataservice IDetc.was added further.
[0117]
The client which received contents information transmits the acquisition request of the right-of-use information (Usage Right) corresponding to receiving contents to a license server (step (23)). Right-of-use information ID (UID) contained in the startup file (refer to drawing 15) previously received from the shop server in this demandLeaf ID as client identification data and transaction ID (TID) contained in

the startup file (refer to drawing 15) previously received from the shop server are contained.
[0118]
A license server will perform order inquiry processing (step (24)) to a managerial systemif the acquisition request of right-of-use information (Usage Right) is received. Right-of-use information ID (UID) and transaction ID (TID) are contained in this demand. The managing server which received order reference transmits the response indication which set up the utilization condition corresponding to right-of-use information ID (UID) as an order reference response to a license server (step (25)).
[0119]
The license server which received the response indication generates the right-of-use information (Usage Right) which set up the contents utilization conditionand publishes it to a client (step (26)). It is constituted by the permit information of various processingssuch as a copy to the reproduction frequency of contentsa termand an external instrumentand check-out processingwith a contents utilization condition.
[0120]
Based on the utilization condition recorded on right-of-use information (Usage Right)the use of contents of the client which received right-of-use information (Usage Right) is attained about the contents which received from the contents server previously. If there is a contents playback demand (step (27)) which specified content ID (CID) and right-of-use information (Usage Right) ID from the userclient application will perform contents playback according to a utilization condition (step (28)).
[0121]
The procedure of fundamental contents playback processing is explained with reference to drawing 19. While contents are provided from the contents server 382 to the client 383 so that I may be understood from the above-mentioned explanationthey are service information and right-of-use information (Usage) as a license from the license server 381 to the client 383.
Right is given.
[0122]
Contents are enciphered by contents key:Kc (Enc (KcContent) and the contents key Kc are keys obtained from the route key Kroot acquirable from EKB.).
[0123]
The client 383 acquires a device node key (DNK) from the service information received from the license serverand EKB of a contents file is decoded based on acquired DNKRoute key : Acquire Kroot and acquired route key:Kroot is used furtherEnc (KrootKc) is decodedcontents key:Kc which acquired and acquired contents key:Kc is boileddecoding processing of enciphered content:Enc (KcContent) is performed morecontents are acquiredand it reproduces.
[0124]
The details of the contents playback processing matched with service information

and right-of-use information (Usage Right) are explained with reference to drawing 20.

[0125]

Drawing 20 is a figure explaining the contents use processing sequence based on the decoding processing of the contents which applied the hard correspondence EKB [EKB (H)] and the service correspondence EKB [EKB (S)].

[0126]

The service information 401 shown in drawing 20 and the right-of-use information 403 are data which carries out license sir baccarat receipt.

The encryption contents file 402 is data received from a contents server.

The service information 401 Leaf ID as a leaf identifierthe version of EKB to applyThe data E (Kroot'SDNK) which enciphered the device node key (SDNK) required for decoding of the service correspondence EKB [EKB (S)] corresponding to service by route key Kroot' set up corresponding to a hard correspondence category tree is stored.

[0127]

The encryption contents file 402 by the service correspondence EKB [EKB (S)] and the route key Kroot which stored the route key Kroot set up corresponding to the category tree corresponding to service Content ID (CID)It is a file containing the data E (KrootCID+Kc) which enciphered the contents key (Kc) applied to contents cipher processing and decoding processingand the data E (KcContet) which enciphered contents (Content) by the contents key Kc.

[0128]

The right-of-use information 403 is the data which stored leaf ID and the utilization condition information of contents. Various utilization conditionssuch as an available term set up corresponding to contentsusing frequencyand copy restrictionsare included in the utilization condition information of contents. The user device which received the right-of-use information 403 stores right-of-use information as security information corresponding to contentsor stores it in AV index file as index data of contents.

[0129]

For examplein the user device with high throughputsuch as a processorwhich has a mass memory measure of PC etc.It is possible to store right-of-use information as security information corresponding to contentsand it is preferred to store all the right-of-use informationand to perform processing which referred to all the right-of-use information on the occasion of contents use. In [on the other handdo not have a mass memory measureand] user devicessuch as a portable device (PD) with low throughputsuch as a processorProcessing of performing processing which stored the right-of-use information 403 which consists of selected information in AV index file as index data of contentsand referred to the utilization condition information in AV index file on the occasion of contents use is possible.

[0130]

In Step S501 shown in drawing 20a user device applies the device node key (HDNK) 412 of hard correspondenceDecoding processing of EKB(H)411 of hard

correspondence is performedand route key Kroot' set up corresponding to a hard correspondence category tree is acquired from EKB(H)411. Processing of EKB which applied DNK turns into processing according to the technique previously explained with reference to drawing 5.

[0131]

Nextin Step S502route key Kroot' taken out from EKB (H) is usedDecoding processing of the encryption data E in the service information 401 (Kroot'SDNK) is performedand the device node key (SDNK) applied to processing (decoding) of the service correspondence EKB [EKB (S)] is acquired.

[0132]

Nextin Step S503the device node key (SDNK) taken out from service information is usedProcessing (decoding) of the service correspondence EKB [EKB (S)] stored in the encryption contents file 402 is performedand the route key Kroot set up corresponding to the category tree corresponding to the service stored in the service correspondence EKB [EKB (S)] is acquired.

[0133]

Nextin Step S504the route key Kroot taken out from the service correspondence EKB [EKB (S)] is usedDecoding processing of the encryption data E (KrootCID+Kc) stored in the encryption contents file 402 is performedand a contents key (Kc) is acquired with content ID (CID).

[0134]

Nextin Step S505matching (collation) processing of the content ID (CID) taken out from the encryption contents file 402 and the content ID stored in right-of-use information is performed. In [if it is checked by conducts matching that use of contents is possible] Step S506The contents key (Kc) taken out from the encryption contents file 402 is appliedenciphered content E (KcContent) stored in the encryption contents file 402 is decodedand contents are reproduced.

[0135]

The hard correspondence EKB as EKB corresponding to the category tree set up corresponding to the hardware as contents use apparatus to have mentioned above [EKB (H)]The service correspondence EKB as EKB corresponding to the category tree set up corresponding to contents use service [EKB (S)] is individually provided to a userrespectivelyand it enables only the user who has just DNK to each EKB to use service.

[0136]

DNK for decoding the service correspondence EKB [EKB (S)]i.e.SDNKIt can provide as the service information 401 corresponding to contentsSince SDNK was considered as the composition enciphered with the application of route key Kroot' set up corresponding to the hard correspondence category tree which can acquire only the apparatus which has DNK corresponding to just hardwarei.e.HDNKOnly the user device which has just HDNK can acquire SDNKand service is used.

[0137]

Since it had composition which performs conducts matching of the content identifier (CID) acquired from the encryption contents file 402and CID acquired

from right-of-use information in contents useIt becomes possible [considering it as the indispensable business of a contents playback process] to acquire the right-of-use information 403 and to store CID informationand contents use according to a utilization condition is realized.

[0138]

Nextprocessing in case processing of client application is the execution application of audition processing is explained with reference to the sequence diagram of drawing 21.

[0139]

In audition processinga contents information file (refer to drawing 19) is acquired as well as content purchase processingand it stores in the storage parts store of a client system.

Thenalthough it is also possible to reproduce by the same processing as purchase contentsthe example which performs streaming reproduction processing is explained with reference to drawing 21without storing in a storage parts store.

[0140]

In streaming audition processing executionclient application performs a contents download request to a contents server (step (31)). This is the contents to which the client gave the audition demand previously. Client application specifies contents by content ID (CID)and performs a contents download request to a contents server.

[0141]

In the case of streaming reproductiona contents server transmits the piece data (contents part) of contents to a client one after another (step (32)). The client which received the KOTENTSU part performs regeneration to receiving contents (step (33))and transmits the demand of a following contents part to a contents server. Streaming reproduction is performed by performing this processing continuously.

[0142]

The procedure of audition regeneration is explained with reference to the flow of drawing 22. In Step S701client application acquires service ID out of the audition contents file which received from the contents server.

[0143]

Nextin Step S702the existence of the default right-of-use information (Default Usage Right) (refer to drawing 17 (b)) corresponding to extracted service ID is judged. Default right-of-use information is right-of-use information transmitted from a license server with service information (refer to drawing 17 (a)) at the time of the registration processing of a client.

It is the right-of-use information which is used to the contents which it can try listening unlike the right-of-use information published corresponding to purchase contents.

[0144]

It is audition execute permission conditions to hold default right-of-use information (Default Usage Right) in a contents auditionWhen default right-of-use information is not heldit progresses to Step S705and contents playback is not performed as an errorbut processing is ended.

[0145]

When default right-of-use information (Default Usage Right) is storedin Step S703default right-of-use information is verified and record of right-of-use information is checked. Audition permission of the contents of audition flag one or the content ID information listening can be tried is stored in default right-of-use informationfor example.

These information is acquired.

[0146]

Nextin Step S704contents are reproduced based on the utilization condition of default right-of-use information (Default UsageRight). Regeneration turns into regeneration accompanied by the decoding processing of the enciphered content which receives from a contents serveras explained with reference to above-mentioned drawing 19 and drawing 20.

[0147]

Also in the audition processing without purchase processing of contentsit is necessary to acquire the key for contents decoding by the key acquisition processing based on EKB processing as well as reproduction of the purchase contents explained with reference to drawing 20. For examplethe hard correspondence EKB as EKB corresponding to the category tree set up corresponding to the hardware as contents use apparatus [EKB (H)]The composition whose execution of contents playback only the user who has just DNK to the service correspondence EKB as EKB corresponding to the category tree set up corresponding to contents use service [EKB (S)] enables is applicableSetting out becomes possible as a range which limited reproduction authority also in the audition.

[0148]

As mentioned abovea client acquires default right-of-use information (Default Usage Right) in the case of the registration processing to a license serverSince it is the composition made not being accompanied by the purchase processing of contentsand possible [based on default right-of-use information / in contents playback] in the case of audition processinga userThe client to which audition reproduction of contents is attained and an audition is permitted without performing the purchase of contentsRegistration processing to a license server is performedand since it will be limited to the client which has default right-of-use informationaudition data is prevented from overflowing disorderly.

[0149]

Although the sequence diagram of drawing 21 showed the example of streaming reproductionIt is also possible to store audition data in the storage of a clientto judge the existence of default right-of-use information (Default Usage Right) at

the time of reproductionand to have composition reproduced based on record of default right-of-use information.
[0150]
[7. Backup / restoration-processing]
Nextthe backup process and restoration processing about contents or contents right-of-use information which the client purchased are explained.
[0151]
Restoration processing is performed as the re acquisition of the time of the content purchase of a client or the license information corresponding to the contents performed as processing after purchasei.e.service informationand right-of-use informationa storing processor re acquisition processing of contents.
[0152]
As a processing modeservice informationright-of-use informationone re acquisition of the contentsor the re acquisition of these data of all the is possible. In the example described belowalthough the re acquisition of service informationright-of-use informationand all the contents data and the example of a storing process sequence are explainedit is possible not only the processing that not necessarily carries out re acquisition of these all data but to carry out re acquisition only of one of the data selectively.
[0153]
The details of backup/restoration processing are explained below with reference to drawing 23. Drawing 23 shows the initial step of the communication sequence in the backup/restoration processing performed between clients which have client application and a browsersuch as PCand a shop servera contents servera license server and a managerial system. Hereafterthe processing shown in a sequence diagram is explained.
[0154]
The client should perform content purchase regularly according to the content purchase processing mentioned above. The sequence shown in drawing 23 is a sequence performed following content purchase.
[0155]
The client which performed content purchase processing generates the restoration-processing demand file [restore.dat] as a data file for acquisition of backup/restoration data (step (50)). The composition of a restoration-processing demand file [restore.dat] is shown in drawing 24.
[0156]
As shown in drawing 24a restoration-processing demand file [restore.dat]It is constituted by the identity data which serves as leaf ID as client identification data in an EKB distribution tree from a hash (hash) value (Message Authentication Code)for exampleMAC. Client application computes the hash value or MAC as data for verification based on leaf ID with the application of the secret key shared with a managerial systemand generates the restoration-processing demand file [restore.dat] which consists of leaf ID and data for verification.
[0157]

A message authenticator (MAC:Message authentication Code) is generated as data for alteration verification of data. The example of MAC value generation using DES cipher-processing composition is shown in drawing 25. (dividing the target message per 8 bytesas shown in the composition of drawing 25 -- the divided message is hereafter set to) M1M2...MN -- exclusive OR of an initial value (Initial Value (hereafter referred to as IV)) and M1 is carried out first (the result is set to I1). NextI1 is put into a DES encryption sectionand it enciphers using a key (hereafter referred to as K1) (an output is set to E1). Continuouslyexclusive OR of E1 and M2 is carried outthe output I2 is put in to a DES encryption sectionand it enciphers using the key K1 (output E2). Hereafterthis is repeated and encryption processing is performed to all the messages. EN which came out at the end serves as a message authenticator (MAC (Message Authentication Code)).

[0158]

If the generator data is changedand a MAC value turns into a different valueperforms comparison with MAC generated based on the data (message) of a verification objectand MAC currently recorded and is in agreementas for the data (message) of a verification objectit will be proved that change and an alteration are not made.

[0159]

It returns to the sequence of drawing 23 and explanation is continued. A client accesses the restoration page which a managerial system provides via a browser (step (51))and a managerial system shows the browser of a client a restoration page (step (52)). The restoration page which a managerial system presents is a page with the function to perform upload processing of a restoration-processing demand file [restore.dat].

[0160]

In the restoration page which a managerial system presentsa client uploads the restoration-processing demand file [restore.dat] which client application generated. A restoration-processing demand file [restore.dat]It is constituted by the hash (hash) value which serves as leaf ID as client identification data in an EKB distribution treefor example from MAC (Message Authentication Code) as explained with reference to drawing 24.

[0161]

If a restoration-processing demand file [restore.dat] is receiveda managerial systemUsing the secret key shared with a clientthe hash value to leaf ID is computedcollation processing of a calculation hash value and a receiving hash value is performedand received data are verified (step (54)). The startup file for backup/restoration is transmitted to a client on condition of a calculation hash value for the receiving hash value having suited (step (55)). The composition of a startup file has the same file organization with having explained with reference to drawing 15 previously.

[0162]

A startup file is passed to client application from a browser (step (56))starts backup/restoration execution program in which distinction selection is made by

description of a startup fileor the extensionand performs restoration processing (step (57)).
[0163]
As a processing object of backup/restoration processingthere are service informationcontentsand contents right-of-use information. Service information can be acquired by the registration processing to a license serveras mentioned aboveand contents can be acquired from a contents server. Right-of-use information is acquired from a license server. Also in backup/restoration processingeach of these data will be acquired from each server.
[0164]
Firstwith reference to drawing 26the acquisition processing of the service information for backup/restoration is explained. Fundamentallythis processing becomes a thing according to the same procedure as the client registration processing at the time of the content purchase explained previously.
[0165]
Firstclient application transmits a registry request to a license server (step (61)). Transaction ID (TID) contained in the startup file which the managerial system generated is contained in this registry request.
[0166]
Based on transaction ID (TID)the license server which received the registry requestIt identifies that it is acquisition of the service information for backup/restorationand the assignment request (step (62)) of service prior datai.e.the data for backup/restoration of service informationis performed to a managerial system. Based on management datait verifies whether a managerial system has the client terminal which performed processing based on the same transaction IDandin a certain casethese are matched and memorized (step (63)). This is because setting out of not performing processing in the processing demand which sets up the maximum (for example3 times) of the processing frequency of backup/restoration processingand exceeds a maximum is enabled.
[0167]
The managerial system which performed the update process of management data transmits a service prior data quota response to a license server (step (64)). This is transmitted as issuing permission information on the service information for backup/restoration.
[0168]
The license server which received the service prior data quota response performs issue processing to the client of the service information for backup/restoration (step (65)). As previously explained with reference to drawing 17 (a)service information to the service information 370. Leaf ID peculiar to the client set up in an EKB distribution treeservice ID as a service identifierthe data that enciphered the device node key (DNK) by the route key (Kroot) furtherand E (KrootDNK) are contained.
[0169]
Default right-of-use information (refer to drawing 17 (b)) is also published from a

license server to a client at the time of this processing. As explained previouslyalthough right-of-use information stores the utilization condition of purchase contents and is usually published corresponding to the purchase of contentsDefault right-of-use information does not publish the purchase of contents as conditionsand publishes registration processing of a clientor issue processing of service information as conditions. This default right-of-use information is applied as effective right-of-use information in the case of audition processing of contentsas mentioned above.

[0170]

The client which received service information and default right-of-use information from the license server is stored in a memory measure by making these data backup (step (66)).

[0171]

Nextwith reference to drawing 27backup/restoration processing of contents are explained. In backup / restoration-processing execution of contentsclient application performs a contents download request to a contents server (step (71)). This is the same as that of the contents which the client purchased previously. Client application specifies contents by content ID (CID)and performs a contents download request to a contents server.

[0172]

A contents server will transmit the contents information corresponding to CID to a clientif a contents download request is received (step (72)). This contents information is information containing enciphered content. Contents data:Enc enciphered by contents key:Kc as previously explained with reference to drawing 17 (c) (KcContent)contents key: -- Kc -- route key: -- they are EKB for acquiring data:Enc (KrootKc) enciphered by Krootand also :route key:Krootand the file to which informationincluding audition flag dataservice IDetc.was added further.

[0173]

The client which received contents information transmits the acquisition request of the right-of-use information (Usage Right) corresponding to receiving contents to a license server (step (73)). Right-of-use information ID (UID) contained in a startup file (refer to drawing 15)leaf ID as client identification dataand transaction ID (TID) are contained in this demand.

[0174]

A license server will perform order inquiry processing (step (74)) to a managerial systemif the acquisition request of right-of-use information (Usage Right) is received. Right-of-use information ID (UID) and transaction ID (TID) are contained in this demand. The managing server which received order reference transmits the response indication which set up the utilization condition corresponding to right-of-use information ID (UID) as an order reference response to a license server (step (75)).

[0175]

The license server which received the response indication generates the right-of-use information (Usage Right) which set up the contents utilization conditionand

carries out a recurrence line (step (76)) to a client. It is constituted by the permit information of various processingssuch as a copy to the reproduction frequency of contentsa termand an external instrumentand check-out processingwith a contents utilization condition.

[0176]

The client which received right-of-use information (Usage Right) stores in a memory measure the contents and the right-of-use information which were received previously as backup data.

[0177]

In backup/restoration processingthe right-of-use information which a license server publishes is good also as what set up a different utilization condition from the right-of-use information published on the occasion of regular content purchase processing. For exampleconditionssuch as restriction of conditions severer than the utilization condition included in the right-of-use information published at the time of regular content purchasefor examplean available termcopy prohibitionor prohibition on check-outmay be set upand setting-out issue of the right-of-use information backup / for restoration processing may be carried out.

[0178]

[8. Secondary distribution] of the contents by a recommendation file

By nextthe thing for which the client which purchased contents regularly performs what is called contents secondary distribution that provides other clients with purchase contentsand newly distributes the contents right of use from a license server. On condition that it has the just contents right of use also in the client which received secondary contents distributingcontents use is enabledand the composition which realized mitigation of the contents distribution load from a contents server is explained further.

[0179]

As mentioned abovethe client which carries out reuse of the contentsIn order to use contentswhile receiving the contents enciphered from the contents serverit is necessary from a license server to receive license informationi.e.service informationand the right-of-use information corresponding to contents.

[0180]

Since license informationi.e.service informationand right-of-use information are data with small data volumeeven if transmission and reception through communications networkssuch as the Internetare performed frequentlythe problem that there are also few rises of traffic and they require great distribution time is not generated. Howeveron the other handcontents will become it is varioussuch as music dataimage dataand a programand big [the data volume]. In transmitting such mass contents to many clients from a specific contents serverair time becomes long and it generates various problemssuch as a burden of a contents serverand a rise of network traffic. The trouble of the contents distribution error by the communication error under communication may also be generated.

[0181]

Other clients are provided with the contents which the client which already

purchased regular contents below holdsThat issecondary distribution is performed and the client which received offer of the contents by secondary distribution explains the system which decreased the load of the contents transmission to the client of a contents server by receiving the license information of the contents from a license server.

[0182]

The flow explaining the procedure which generates the contents file to which the client received regularly provides other clients with contents is shown in drawing 28. The data file containing the contents with which other clients are provided is called a recommendation file. The explanation file (for exampleHTML file) of the contents is included in a recommendation file the contents file containing the enciphered contents and if needed.

[0183]

The process flow of drawing 28 is explained. The client which performs processing of drawing 28 is a client which performed content purchase processing mentioned abovereceived the client which purchased contents regularlyor the recommendation file from other clientsand acquired the regular license in a subsequent procedure. Processing of drawing 28 is performed under control by the control means (CPU etc.) of the information processor as a client system as one execution program of client application (client application 12 of drawing 1). In Step S801a client displays a recommendation file creation screen on the display of a self client apparatus.

[0184]

The example of a recommendation file creation screen is shown in drawing 29. A client carries out regular purchasewhen the refreshable contents list 651 is displayed in the center and generates a recommendation filecontents are chosen from this contents list 651 (Step S802)and a title etc. are displayed on the right-hand side list 654. Moving processing between the contents list 651 and the list 654 is performed by operation of the transfer switches 652 and 653.

[0185]

In Step S803selection of the contents for recommendation file generating will push the recommendation file creation button 655. In Step S804a push on the recommendation file creation button 655 will choose whether generation storing of the explanation file which combined with the KONTEN file in the recommendation fileand was described by the explanation filefor exampleHTMLis carried out. It is [this] arbitrarily selectable in a user.

[0186]

As it is indicated in drawing 30 (b) as recommendation file 720 composition which combined with the recommendation file the contents file 721 containing enciphered content and the contents explanation file 722 as shown in drawing 30 (a)There are two modes with recommendation file 730 composition which consists only of the contents file 721 containing enciphered contentand a client becomes selectable freely about the mode.

[0187]

In Step S804when the file for contents explanation was not created and it choosesthe recommendation file 730 which consists only of the contents file 721 shown in drawing 30 (b) is generated.
[0188]
The composition of a contents file is shown in drawing 31. The content ID (CID) as shop server URL which indicates the meta information as contents additional information and the shop in which content purchase is still more possible to be enciphered contentand a content identifier is contained in the contents file (MQT file) 721.
[0189]
The enciphered content stored in a contents file is the contents enciphered by the contents key Kc.
The contents key Kc is a key acquirable only by application of a key acquirable by decoding of the validation key blocks (EKB) provided with the application of validation key-blocks (EKB) distribution tree composition.

[0190]
On the other handin Step S804when the file creation for contents explanation is chosenit progresses to Step S806 and the explanation data (metadata) for contents explanation file (HTML file) generation is acquired from a contents management table. The contents explanation data corresponding to contents is stored also in the contents file with enciphered contentas mentioned abovebut. The client which acquired the contents right of use regularly is carrying out storing management at another file by using as contents managing data metadata corresponding to the contents taken out from philharmonic contents.
The metadata for an explanation file generated in a recommendation file is extracted from this contents managing data.

[0191]
In Step S807the metadata extracted from contents managing dataProcessing stuck on the template HTML file set as client application is performedthe HTML file for explanation corresponding to contents is generatedand the recommendation file which consists of a contents file and a HWML file for explanation is generated in Step S808.
[0192]
The example of a display configuration of the HTML file as data for contents explanation is shown in drawing 32. The example shown in drawing 32 is an example in case contents are music data. As the file for explanation is shown in drawing 32the explanation about information listssuch as a musical piece title of a music contentan artistand a distributorfurther various kinds of operationsand processing is described. The client which received the recommendation file from other clients will open this explanation file first.
[0193]
The contents stored in the recommendation file are the enciphered contentsand

when regular license informationi.e.the right-of-use information on service information and contents correspondenceis not acquiredthey cannot be reproduced. Thereforewhen the client which received the recommendation file uses the contents stored in the recommendation fileprocedure which acquires license information will be performed.

[0194]

This license information acquisition processing is explained with reference to the process flow of drawing 33 and drawing 34. The client which received the recommendation file opens the file for explanation (HTML file) shown in drawing 32and clicks an audition and the purchase contents distribution site button 731 (Step S811). By this click processingclient application starts (Step S812) and the contents file (MQT file) (refer to drawing 31) stored in the same recommendation file is readContent ID (CID) and shop URL are extracted from a contents file (Step S813).

[0195]

Thusthe audition of the file for contents explanation and the purchase contents distribution site button 731Shop server URL is extracted from a contents fileand it is constituted as link data which starts the client application program which performs processing which outputs extraction URL to a browser. Thereforeit enables it for the client which received the recommendation file to connect with a shop easilyand to perform purchase procedure.

[0196]

In Step S814a contents file name is set up based on the content ID (CID) extracted from the contents file. This is performed as file name setting processing beforehand set up in client applicationfor examplethe title of contentsan artist nameor its complex data is applied. In Step S815the KONTEN file of the file name set up at Step S8145 is stored in the storage parts store of a client.

[0197]

Nextin Step S816shop URL extracted from the contents file at Step S813 is passed to a browserand a browser reads the shop page corresponding to receipt URL from a shop server.

[0198]

In Step S831 of the process flow of drawing 34a shop screen is displayed on the display of a client. The processing which that of the following processings is the same as either processing of the purchase processing of contents mentioned above and audition processing fundamentallyand was previously explained according to drawing 11drawing 13drawing 18and drawing 21 will be followed. howeverfinishing [the contents themselves / concentrated rye ANTO / a recommendation file to acquisition] already -- it is -- since -- a contents sir -- foolish --- ** -- contents receipt processing is omitted.

[0199]

The outline of a series of processings serves as processing shown in less than step S832 of the process flow of drawing 34. Firstif a client specifies purchase in the shop screen which a shop server presents and outputs a purchase request to

a shop serverthe startup file for purchase will be transmitted from a shop server. This has previously the same composition as the startup file explained with reference to drawing 15.
[0200]
Nextin Step S833the content ID (CID) as a content identifier is acquired from a startup file. Nextin Step S834a contents file name is computed based on content ID (CID). As explanation of the flow of previous drawing 33 described the contents file name at the time of storing contents in a client apparatusbeing set up based on content ID (CID) is specified in client applicationand matching of CID and a file name is made.
[0201]
In Step S835the file of the same file name as the file name computed from content ID (CID) judges whether it is stored in the storage parts store of a self client apparatus. When contents are not storedit will progress to Step S837it will connect with a contents serverand contents download will be performed. This processing is the same as the processing at the time of the content purchase explained previously.
[0202]
Howeverthe client which has received the recommendation file stores in a storage parts store the contents file which set up the predetermined file name in Step S814 of flow ** of previous drawing 33and S815.
The download processing of contents is omitted and it becomes possible to perform acquisition processing of the contents right-of-use information on Step S836and to end processing.

[0203]
When a client performs contents playbackas mentioned abovecollation with the content identifier (CID) stored in contents right-of-use information and the content identifier (CID) of reproduction object contents is performedand contents playback is performed on condition of coincidence of CID. The contents key Kc is acquired by decoding of the validation key blocks (EKB) provided with the application of validation key-blocks (EKB) distribution tree compositionBy performing decoding processing of enciphered content with the application of the acquired contents key Kcit becomes possible to carry out reuse of the contents.
[0204]
By thusthe thing for which the client for which contents are already held provides other clients with the contents file containing enciphered content and the recommendation file which consists of a file for explanation. Other clients become possible [receiving contents without access to a contents distribution server]. Since it is the composition whose use of contents is attained on condition that other clients acquire right-of-use informationuse of inaccurate contents is prevented.
[0205]
Although it has omitted about the acquisition processing of service information in

the flow of drawing 34When the client which does not hold service information receives a recommendation fileaccess to a license server is performedregistration processing is performedand it is necessary to acquire service information. This registration processing procedure serves as processing corresponding to the processing previously explained with reference to drawing 13 and drawing 16.
[0206]
As mentioned aboveit has explained in detail about this inventionreferring to a specific example. Howeverit is obvious that a person skilled in the art can accomplish correction and substitution of this example in the range which does not deviate from the gist of this invention. That iswith the gestalt of illustrationthis invention has been indicated and it should not be interpreted restrictively. In order to judge the gist of this inventionthe column of the claim indicated at the beginning should be taken into consideration.
[0207]
A series of processings in which it explained into the specification can be performed by the composite structure of hardwaresoftwareor both. When performing processing by softwarethe program which recorded the processing sequenceIt is possible to install in the memory in the computer built into hardware for exclusive useand to make it performor to make the general purpose computer which can perform various processing install and execute a program.
[0208]
For examplea program is recordable on the hard disk and ROM (Read OnlyMemory) as a storage beforehand. A program Or a flexible diskCD-ROM (Compact Disc Read Only Memory)It is temporarily or permanently storable in removable recording mediasuch as MO (Magneto optical) diskDVD (Digital Versatile Disc)a magnetic diskand semiconductor memory (record). Such a removable recording medium can be provided as what is called a software package.
[0209]
Install a program in a computer from a removable recording medium which was mentioned aboveand also. From a download sitevia networks [**** / carrying out radio transmission]such as LAN (Local Area Network) and the Internetto a computerIt transmits to a computer with a cableand in a computerit can receive and the program transmitted by making it such can be installed in storagessuch as a hard disk to build in.
[0210]
Various kinds of processings written in the specification may be performed in parallel or individually [the throughput or if needed] for a device of a time series not only performingbut performing processing according to a statement.
[0211]
[Effect of the Invention]
As mentioned aboveas explainedaccording to the composition of this inventiona clientDefault right-of-use information (Default Usage Right) is acquired in the case of the registration processing to a license serverBased on default right-of-use informationcontents playback is permitted in the case of the audition processing

without purchase processing of contentsand the audition reproduction of contents of a user is attainedwithout performing the purchase of contents. The client to which an audition is permitted performs registration processing to a license serverand since it will be limited to the client which has default right-of-use informationaudition data is prevented from overflowing disorderly.

[0212]

Also in the audition processing without [according to the composition of this invention] purchase processing of contentsThe hard correspondence EKB as EKB corresponding to the category tree set up corresponding to the hardware as contents use apparatus [EKB (H)]The composition whose execution of contents playback only the user who has just DNK to the service correspondence EKB as EKB corresponding to the category tree set up corresponding to contents use service [EKB (S)] enables is applicableSetting out becomes possible as a range which limited reproduction authority also in audition processing.

[Brief Description of the Drawings]

[Drawing 1]It is a figure showing the outline of the contents providing system which applied this invention.

[Drawing 2]It is a figure showing a client and each serverand the example of composition of a managerial system.

[Drawing 3]It is a tree lineblock diagram explaining various key and data encryption processing and distribution processing.

[Drawing 4]It is a figure showing the example of the validation key blocks (EKB) used for distribution of various keys and data.

[Drawing 5]It is a figure showing the example of distribution which uses the validation key blocks (EKB) of a contents keyand the example of decoding processing.

[Drawing 6]It is a figure showing the example of a format of validation key blocks (EKB).

[Drawing 7]It is a figure explaining the composition of the tag of validation key blocks (EKB).

[Drawing 8]It is a figure explaining the category division in tree composition.

[Drawing 9]It is a figure explaining the category division in tree composition.

[Drawing 10]It is a figure explaining the example of the category division in tree composition.

[Drawing 11]It is a figure showing the executive operation sequence (the 1) between each entity in content purchase or audition processing.

[Drawing 12]It is a flow chart showing the transaction ID generation performed in a managerial systemand an issue processing procedure.

[Drawing 13]It is a figure showing the executive operation sequence (the 2) between each entity in content purchase or audition processing.

[Drawing 14]It is a flow chart showing the download permission procedure performed in a managerial system.

[Drawing 15]It is a figure showing the example of a data configuration of a startup file.

[Drawing 16]It is a flow chart showing the application execution procedure based on the startup file performed in a client.
[Drawing 17]It is a figure showing the example of a data configuration of service information and right-of-use information.
[Drawing 18]It is a figure showing the executive operation sequence between each entity in content purchase processing.
[Drawing 19]It is a figure explaining the outline of contents playback processing.
[Drawing 20]They are contents decoding which applied validation key blocks (EKB)and a figure explaining the example of use processing.
[Drawing 21]It is a figure showing the executive operation sequence between each entity in contents audition processing.
[Drawing 22]It is a figure explaining the outline of audition contents playback processing.
[Drawing 23]It is a figure showing the processing sequence (the 1) between each entity in a licenseor backup/restoration processing of contents.
[Drawing 24]It is a figure showing the example of composition of a restoration-processing demand file [restore.dat].
[Drawing 25]It is a figure showing MAC generation processing composition.
[Drawing 26]It is a figure showing the processing sequence (the 2) between each entity in a licenseor backup/restoration processing of contents.
[Drawing 27]It is a figure showing the processing sequence (the 3) between each entity in a licenseor backup/restoration processing of contents.
[Drawing 28]It is a figure showing the generation processing flow of a recommendation file.
[Drawing 29]It is a figure showing a recommendation file generating screen.
[Drawing 30]It is a figure showing the example of recommendation file organization.
[Drawing 31]It is a figure showing the example of composition of the contents file stored in a recommendation file.
[Drawing 32]It is a figure showing the display example of the contents explanation file stored in a recommendation file.
[Drawing 33]It is a figure showing the license information acquisition processing flow (the 1) in the client which received the recommendation file.
[Drawing 34]It is a figure showing the license information acquisition processing flow (the 2) in the client which received the recommendation file.
[Description of Notations]
10 Client
11 Browser
12 Client application
21 Shop server
22 License server
23 Contents server
31 Managerial system
100 Timer
101 CPU(Central processing Unit)

102 ROM(Read-Only-Memory)
103 RAM(Random Access Memory)
104 Encryption decoding part
105 Codec part
106 Input part
107 Outputting part
108 Storage parts store
109 Communications department
110 Drive
111 Bus
112 Input/output interface
121 Removable recording medium
201 Version
202 Depth
203 Data pointer
204 Tag pointer
205 Signature pointer
206 Data division
207 Tag part
208 Signature
301 Route key
302 Node key
303 Leaf key
304 Category node
350 Root node
351 T system node
352 T service node
353 T hard node
354 Service provider node
355 Leaf
360 Startup file
370 Service information
371 Right-of-use information
372 Contents
373 Audition flag
381 License server
382 Contents server
383 Client
384 Contents
401 Service information
402 Encryption contents file
403 Right-of-use information
411 EKB(H)
601 Restoration-processing demand file

651 Contents list
652653 Switch
653 Recommendation file creation button
654 List
720730 Recommendation file
721 Contents file
722 Contents explanation file
731 An auditiona purchase contents distribution site button

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a figure showing the outline of the contents providing system which applied this invention.
[Drawing 2]It is a figure showing a client and each serverand the example of composition of a managerial system.
[Drawing 3]It is a tree lineblock diagram explaining various key and data encryption processing and distribution processing.
[Drawing 4]It is a figure showing the example of the validation key blocks (EKB) used for distribution of various keys and data.
[Drawing 5]It is a figure showing the example of distribution which uses the validation key blocks (EKB) of a contents keyand the example of decoding processing.
[Drawing 6]It is a figure showing the example of a format of validation key blocks (EKB).
[Drawing 7]It is a figure explaining the composition of the tag of validation key blocks (EKB).
[Drawing 8]It is a figure explaining the category division in tree composition.
[Drawing 9]It is a figure explaining the category division in tree composition.
[Drawing 10]It is a figure explaining the example of the category division in tree composition.
[Drawing 11]It is a figure showing the executive operation sequence (the 1) between each entity in content purchase or audition processing.
[Drawing 12]It is a flow chart showing the transaction ID generation performed in a managerial systemand an issue processing procedure.
[Drawing 13]It is a figure showing the executive operation sequence (the 2) between each entity in content purchase or audition processing.
[Drawing 14]It is a flow chart showing the download permission procedure performed in a managerial system.
[Drawing 15]It is a figure showing the example of a data configuration of a startup file.
[Drawing 16]It is a flow chart showing the application execution procedure based on the startup file performed in a client.

[Drawing 17]It is a figure showing the example of a data configuration of service information and right-of-use information.
[Drawing 18]It is a figure showing the executive operation sequence between each entity in content purchase processing.
[Drawing 19]It is a figure explaining the outline of contents playback processing.
[Drawing 20]They are contents decoding which applied validation key blocks (EKB)and a figure explaining the example of use processing.
[Drawing 21]It is a figure showing the executive operation sequence between each entity in contents audition processing.
[Drawing 22]It is a figure explaining the outline of audition contents playback processing.
[Drawing 23]It is a figure showing the processing sequence (the 1) between each entity in a licenseor backup/restoration processing of contents.
[Drawing 24]It is a figure showing the example of composition of a restoration-processing demand file [restore.dat].
[Drawing 25]It is a figure showing MAC generation processing composition.
[Drawing 26]It is a figure showing the processing sequence (the 2) between each entity in a licenseor backup/restoration processing of contents.
[Drawing 27]It is a figure showing the processing sequence (the 3) between each entity in a licenseor backup/restoration processing of contents.
[Drawing 28]It is a figure showing the generation processing flow of a recommendation file.
[Drawing 29]It is a figure showing a recommendation file generating screen.
[Drawing 30]It is a figure showing the example of recommendation file organization.
[Drawing 31]It is a figure showing the example of composition of the contents file stored in a recommendation file.
[Drawing 32]It is a figure showing the display example of the contents explanation file stored in a recommendation file.
[Drawing 33]It is a figure showing the license information acquisition processing flow (the 1) in the client which received the recommendation file.
[Drawing 34]It is a figure showing the license information acquisition processing flow (the 2) in the client which received the recommendation file.
[Description of Notations]
10 Client
11 Browser
12 Client application
21 Shop server
22 License server
23 Contents server
31 Managerial system
100 Timer
101 CPU(Central processing Unit)
102 ROM(Read-Only-Memory)
103 RAM(Random Access Memory)

104 Encryption decoding part
105 Codec part
106 Input part
107 Outputting part
108 Storage parts store
109 Communications department
110 Drive
111 Bus
112 Input/output interface
121 Removable recording medium
201 Version
202 Depth
203 Data pointer
204 Tag pointer
205 Signature pointer
206 Data division
207 Tag part
208 Signature
301 Route key
302 Node key
303 Leaf key
304 Category node
350 Root node
351 T system node
352 T service node
353 T hard node
354 Service provider node
355 Leaf
360 Startup file
370 Service information
371 Right-of-use information
372 Contents
373 Audition flag
381 License server
382 Contents server
383 Client
384 Contents
401 Service information
402 Encryption contents file
403 Right-of-use information
411 EKB(H)
601 Restoration-processing demand file
651 Contents list
652653 Switch

653 Recommendation file creation button
654 List
720730 Recommendation file
721 Contents file
722 Contents explanation file
731 An auditiona purchase contents distribution site button